hw

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	1003.10	2528

53953 7590 03/23/2006

DAVIS LAW GROUP, P.C.
9020 N. CAPITAL OF TEXAS HWY.
BUILDING 1, SUITE 375
AUSTIN, TX 78759

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/647,644	**Applicant(s)** OBRECHT ET AL.	
	Examiner Arezoo Sherkat	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 August 2003_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-104_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-104_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _25 August 2003_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _8/03,3/04,8&9/05_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-104 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-104 are rejected under 35 U.S.C. 102(b) as being anticipated by Hill et al., (U.S. Patent No. 6,088,804 and Hill hereinafter).

3. Regarding claims 1-5, 13, 21, 41, 49, and 95-97, Hill discloses a method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program and (b) searching for information in the information handling system about the code or program, the detection routines including valid program detection routines and malicious code detection routines (col. 4, lines 5-61);

applying the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines, and determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights (i.e., attack severity 61 is a level of security breach that one of simulated attacks 52 could cause computer network 22), and wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score (i.e., security events are presented in database 48 in a column 58 as a percentage of security events per event type)(col. 5, lines 20-67 and col. 6, lines 61-23).

4. Regarding claims 6-12, 14-20, 22-25, 42-48, 50-53, 62-68, 70-76, 78-81, 88-94, and 98-104, Hill discloses wherein the valid program detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program (i.e., the examined code not matching any of the training signatures 53), and wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with malicious code (col. 5, lines 21-65).

5. Regarding claims 28-31, 56-59, and 84-85, Hill discloses wherein the detection routines access information about the executable code under investigation from an operating system of the information handling system via Application Programming Interfaces (APIs), and the detection routines gather information from executable code or a program by examining a binary image of the executable code or program (col. 5, lines 20-67 and col. 6, lines 61-23), the characteristics and behavior of the executable code or program, and any other related code or programs used by the executable code under investigation (i.e., security events may include port scans, malicious softwares, penetration attempts, and others that are identified through either a specific code signature or through actions or attempts at actions)(col. 4, lines 10-52).

6. Regarding claims 32, 60, and 86, Hill discloses delivering malicious code detection code (MCDC) containing the detection routines to the information handling system in a small compact code module via at least one of the following: a computer network, Internet, intranet, extranet, modem line, and prepackaged computer readable storage media (col. 4, lines 5-41).

7. Regarding claims 33, 61, and 87, Hill discloses wherein the characteristics and behaviors (i.e., security events) include at least one of the following: logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling the display screen (i.e., security events may include port scans, malicious softwares, penetration attempts, and others that are identified through

either a specific code signature or through actions or attempts at actions)(col. 4, lines 10-52).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 26-27, 54-55, and 82-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al., (U.S. Patent No. 6,088,804 and Hill hereinafter), in view of Arnold et al., (U.S. Patent No. 5,440,723 and Arnold hereinafter).

9. Regarding claims 26-27, 54-55, and 82-83, Hill discloses wherein the scoring algorithm determines a malicious code by detecting occurance of security events (col. 4, lines 30-62).

Hill does not expressly disclose wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold.

However, Arnold discloses wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Hill with teachings of Arnold because it would allow to include scoring algorithm determines a valid/malicious program by a summation of weights of the valid/malicious program detection routines being greater than a corresponding weight threshold as disclosed by Arnold. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Arnold to provide the ability to detect presence of computer viruses which have not been programmed to be detected expilicitly (Arnold, col. 1, lines 64-67).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chess et al., (U.S. Patent No. 6,772,346),

Saman, (U.S. Publication No. 2003/0177397),

Cox et al., (U.S. Patent No. 6,842,861),

Sampath et al., (U.S. Patent No. 6,266,774), and

Bullock et al., (U.S. Publication No. 2005/0137980).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CHRISTOPHER REVAK
PRIMARY EXAMINER
3\18\06

A.S.
A. Sherkat
Patent Examiner
Group 2131
March 17, 2006